

FIG. 1

TOP SECRET//COMINT 04591

20

INITIAL SOFTWARE PRODUCT ~21

MANUFACTURER:

GENERATE ENCRYPTION **KEY A** ~22

GENERATE ONE OF EITHER **SPLIT A** OR **TOKEN** ~24

CALCULATE OTHER OF **SPLIT A** OR
TOKEN USING **KEY A** SUCH THAT
 $SPLIT\ A + TOKEN = KEY\ A:$
 $\therefore SPLIT\ A = KEY\ A \oplus TOKEN$ ~25

ENCRYPT INITIAL SOFTWARE
PRODUCT WITH **KEY A** ~26

INSTALL INITIAL SOFTWARE PRODUCT
AND **SPLIT A** IN HARDWARE PRODUCT ~28

DELIVER **TOKEN** AND
HARDWARE PRODUCT TO CUSTOMER ~29

CUSTOMER:

INSERTS **TOKEN** ~30

HARDWARE PRODUCT COMBINES TOKEN
 \oplus SPLIT A TO PROVIDE **KEY A** ~32

HARDWARE PRODUCT USES **KEY A**
TO DECRYPT INITIAL SOFTWARE ~34

FIG. 2

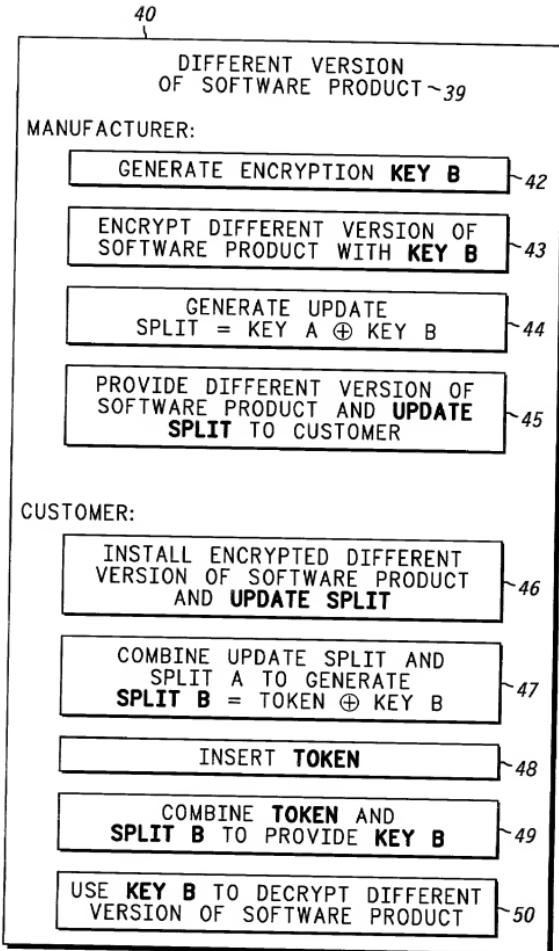


FIG. 3